XXIII. Fiatal Műszakiak Tudományos Ülésszaka, 2018. Kolozsvár, 211–214.
http://eda.eme.ro/handle/10598/30332

INTELLIGENS FŰTÉSI RENDSZER SEBEZHETŐSÉGÉNEK VIZSGÁLATA

VULNERABILITY ANALYSIS OF A SMART HEATING SYSTEM

Sándor Barnabás

Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 1034, Magyarország Budapest, Bécsi út 96/B; Telefon: +36-1-666-5300, sandor.barnabas@gmail.com

Abstract

The opportunities offered by the smart city and the smart home to create livelier cities and homes in the increasingly populous cities. [1] At the same time, there may be more problems that the average user does not think yet. It will be of utmost importance for information security and IT security, as the development of technology may not be able to keep up with the society that uses them. On a theoretical and practical level, I examine an intelligent heating system for IT vulnerability, as well as some cases of attacks against IoT in recent years.

***Keywords**: smart city, smart home, smart heating, vulnerability.*

Összefoglalás

Az okos város és az okos otthon által nyújtott lehetőségek, mellyel élhetőbb városokat, otthonokat alakíthatunk ki az egyre népesebb nagyvárosokban. [1] Ezzel egyidejűleg azonban több olyan probléma is bekövetkezhet, amire egyelőre még az átlagfelhasználó nem gondol. Kiemelkedő jelentősége lesz az információbiztonság és az informatikai biztonság területének, mivel a technológia fejlődésével nem feltétlenül tud lépést tartani az ezeket felhasználó társadalom. Elméleti és gyakorlati síkon vizsgálok egy intelligens fűtésrendszert az informatikai sebezhetőség szempontjából, továbbá ismertetek néhány esetet az elmúlt években elkövetett IoT elleni támadások közül.

***Kulcsszavak:** okos város, okos otthon, okos fűtés, sebezhetőség, károkozás.*

1. Bevezetés

Az IoT ellen elkövetett támadások közül az elmúlt évek legjelentősebb támadása a Mirai botnet támadás volt 2016. október 21-én, ahol több millió eszköz, többek között fertőzött IP kamerák, routerek, DVR egységek támadták a Dyn Inc. DNS szolgáltatásait, ezzel több nemzetközi cég szolgáltatása vált elérhetetlenné. A legnagyobb cégek melyek érintettek voltak a támadás során: Amazon, Netflix, Twitter, Spotify, Reddit, CNN, PayPal, Pinterest, Fox News, de a New York Times, The Guardian és a Wall Street Journal kiadók is. [2][3]

A támadás volumenét az is mutatja, hogy elemzések alapján nagyjából 1,2 millió fertőzött eszközről érkezett egyidőben 100 Gbps forgalmat generáló HTTP lekérés a Dyn szerverei felé közel 164 országból. [4]

2. Sebezhetőség vizsgálat

A vizsgálat célja a Honeywell Y87RF vezeték nélküli termosztát rendszer interne-

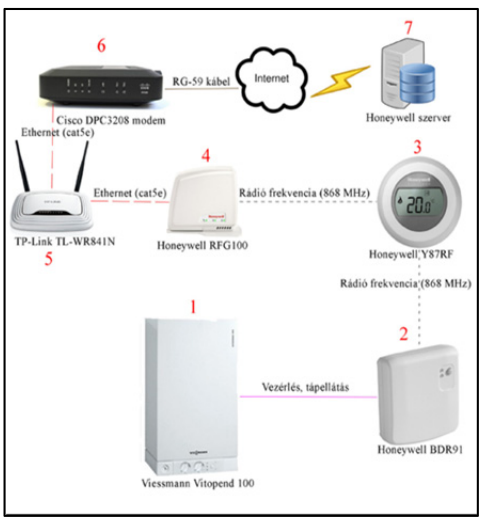
tes átjárójának, a Honeywell RFG100 informatikai sérülékenységének feltárása és azok kihasználása volt. A vizsgálat során az alábbi célok kerültek megfogalmazásra:

- A Honeywell RFG100 internetes átjáró sérülékenységeinek feltárása;
- Lehetséges károkozási módok informatikai, gazdasági és személyi szempontból;
- Védelmi javaslatok, megoldások megfogalmazása.

2.1. A rendszer működési elve

Az intelligens fűtésrendszer kényelmi okokat szolgál. A helyszín egy balatoni nyaraló, ahol nincs folyamatos jelenlét, így például egy téli odautazás előtt, távolról bekapcsolva a fűtést, kellemes meleg fogadja az odaérkezőket.

Működéséhez a Honeywell egyzónás termosztát csomag szükséges, illetve internet hozzáférés és használat függvényében okostelefon (iOS vagy Android) vagy asztali számítógép. A rendszer interneten keresztül, bárhonnan a világból vezérelhető, telefonos applikációról, vagy egy weboldalra történő bejelentkezés után. Az *1. ábrán* látható a jelenleg működő rendszer blokkvázlata.



1. ábra. *Blokk- és kábelezési vázlat [5]*

2.2. Vizsgálat ismertetése

A „grey box” sérülékenység vizsgálat elsődleges célja a Honeywell RFG100 internetes átjáró által ki- és bemenő hálózati forgalom elfogása, dekódolása, esetleges manipulációja volt. [6] Felhasznált eszközök:

- MikroTik RB951G-2HnD programozható router;
- MacBook Air 13” laptop (Modell: A1466);
- Lenovo ThinkPad x201 laptop;
- WireShark – hálózati csomaganalizáló szoftver;
- Nmap – hálózatvizsgáló szoftver;
- SSLsplit – SSL tanúsítványhamisító szkript;
- ARPspoof – ARP támadásra alkalmas szkript.

2.3. Vizsgálat menete

A TP-Link TL-WR841N routert (**1. ábra**-5) lecseréljük egy programozható MikroTik RB951G-2HnD routerre, így magasabb szintű hálózatirányítási műveleteket hajthatunk végre, majd a „Packet Sniffer” modul segítségével a Honeywell internetes átjáró forgalmát tükröztük és átirányítottuk a Lenovo ThinkPad x201-en futó WireShark célszoftverbe monitorozás céljából. A Honeywell RFG100 internetes átjáró MAC címét kiszűrve célzottan került elemzésre a hálózati forgalom. A hálózati forgalom elemzésekor átfogóbb képet kaptunk arról, hogy az eszköz pontosan milyen adatcsomagokat küld és fogad, illetve, hogy milyen szerverekkel kommunikál. [7]

1. táblázat. *Szerverek, melyekkel az eszköz kommunikál*

CNAME	IP
dns1.honeywell.com	199.64.220.7
dns1.honeywell.com	199.61.24.26
tccprod01.honeywell.com	199.62.84.151
tccprod01.honeywell.com	199.62.84.152
tccprod01.honeywell.com	199.62.84.153

Az **1. táblázat**ban látható szerverek küldik és fogadják az összes csomagot, amik a fűtési rendszer vezérléséért felelnek. Tekintettel arra, hogy az átjárónak nincs kezelőfelülete, illetve nem tudtunk programkód szinten hozzáférni, így az feltételezhető, hogy előre beprogramozott szerverekkel kommunikál. A csomagokat titkosítva a 443-as porton keresztül fogadja, saját belső portjain (50103, 52575, 53200, 55615, 55879, 56475, 59134, 59878, 60410, 61038, 61667, 62575, 64029), melyeket csak a kommunikáció alkalmával nyit ki.

2.4. Szoftveres vizsgálat

A szoftveres vizsgálat során Nmap, Zenmap és SSLsplit vizsgálatot végeztünk, mely során feltárásra került, hogy az alapvető TCP/UDP portokra, mint FTP (20, 21), SSH (22), TELNET (23), WEB (80, 8080), DNS (53), illetve 1-től 10000-ig, nincsenek alapesetben nyitva. Az SSL tanúsítványhamisítás közben pedig az eszköz standby módba kapcsolta magát és lecsatlakozott a hálózatról. Ez arra enged következtetni, hogy ellátták HSTS védelemmel. [8]

2.5. Fizikai vizsgálat

A fizikai vizsgálat során leszerelésre került az eszköz borítása, mely egy SUI ML-2 94V-0 alaplapra épül, melyet egy Atmel AT91SAM9635-CU típusszámú vezérlő chip kontrollál. A fizikai vizsgálat további jövőbeni kutatásokat igényel.

3. Károkozási lehetőségek

Károkozás történhet információbiztonsági szempontból (adatlopás); személy-, vagyon elleni károkozás/bűncselekmény, vagy rongálási szándék alapján. A kutatás rávilágít arra, hogy amennyiben nem megfelelően védett és konfigurált hálózati elemeket alkalmazunk, úgy azon rendszerek további támadások előkészületei is lehetnek, amelyekkel súlyos anyagi károkat lehet okozni. Néhány példával szemléltetve:

Egy gyógyszerraktár eseten pár tized fokos hőmérsékletkülönbség is jelentős lehet az alapanyagok szavatossága kapcsán. Így például, ha egy ottani termosztát rendszert megtámadnak és megemelik, vagy lecsökkentik a hőmérsékletet, súlyos anyagi vagy egészségi károk okozhatók így.

Egy védett objektumnál, hasonló támadás esetén arra „kényszeríthetik” a vagyonőrt, hogy szellőztessen, mivel a szobahőmérséklet át lett állítva 30 fokra. Így egy nyitott nyílászárón keresztül be lehet jutni az épületbe.

Legsúlyosabb esetek között említhető a babamonitor kamerák feltörése, melyek a legismertebb információbiztonsági sérülésekkel rendelkeztek. Sok esetben távolról hozzáfértek a támadók az élő képhez, így kifigyelhették, mikor nincs a közelben senki. Így éjszaka vagy nappal elrabolhatták a védtelen kisgyermekeket. [9]

Elfordult már olyan eset is ahol szívritmus-szabályozók ellen intéztek támadást, hiszen ebben az esetben a használója egészségügyi állapotát lehet vele közvetlenül befolyásolni. [10]

4. Megelőzési javaslatok

Elsődleges megelőzési lépés minden esetben a tájékozódás, hiszen általános probléma, hogy a legolcsóbbat keresik az átlagfelhasználók egy adott eszköz kapcsán. Eszközvásárlás előtt mindenképpen érdemes rákeresni az eszköz típusszámára, illetve az interneten fellelhető bejegyzésekre, cikkekre vele kapcsolatban, mivel elképzelhető, hogy vannak ismert sérülékenységei. Fontos kideríteni, hogy a gyártó meddig vállalja az eszköz szoftveres támogatását. Hiszen, ha már évek óta nincs rá alkalmazás / firmware frissítés, akkor nagy eséllyel nem is fog készülni rá a közeljövőben, ami szintén problémát jelent biztonsági szempontból. Szakemberek folyamatosan foglalkoznak az eszközök sérülékenységének vizsgálatával, így szinte napról-napra

jelennek meg sebezhetőségek. Ebből kiindulva, már egy akár néhány hónapja nem frissített eszköz is kockázatot jelenthet. Természetesen előfordulnak olyan első napi (zero day) sérülékenységek, melyek évek óta jelen vannak a rendszerekben, de még nem fedezte fel azokat senki. Ezek nagy kockázatot jelentenek minden esetben, hiszen rengeteg eszközt érinthetnek világszerte.

5. Összegzés

Összegezve, egyértelműen kijelenthető, hogy a nem megfelelő biztonsággal rendelkező és nem körültekintően telepített rendszerekkel, személy és vagyon elleni károkat lehet okozni. A szakértők bevonása mellett fontos, hogy a felhasználók képezzék magukat az eszközök biztonságos használata, illetve a saját biztonságtudatosságuk érdekében. Nem elég ezeket az eszközöket telepíttetni, meg kell tanulni megfelelően használni és élni velük.

A kutatás elkészítése során felhasználásra és feldolgozásra került a szakirodalomban és az interneten fellelhető tudományos és szakmai anyagok a sérülékenységekkel és azok vizsgálatával kapcsolatban. Alkalmazásra kerültek különböző sérülékenységvizsgáló eszközöket és szoftvereket, melyekkel a kitűzött célokat sikerült teljesíteni.

A vizsgálatok során megállapításra került, hogy a rendszer védett az adott támadási módokkal szemben. Az alapvető hálózati portok kizárólag kommunikáció során kerülnek kinyitásra, illetve az SSL tanúsítványhamisítással szemben is rendelkezik védelemmel.

A kutatást a jövőben mélyebb fizikai és szoftveres vizsgálatokkal folytatjuk, így vezérlő egység szinten is megvizsgálásra kerül az eszköz, továbbá a rádiófrekvenciás kommunikációt is szeretnénk mélyebb tesztek alá vetni.

Szakirodalmi hivatkozások

[1] MTA RKK NYUTI, IBM Magyarország Kft.: *„Smart cities" tanulmány,* 2011. május, ISBN 978-963-08-1739-4

[2] Sam Thielman, Chris Johnston: *Major cyber attack disrupts internet service across Europe and US*, The Guardian, www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service

[3] The Hacker News, Mohit Kumar: Mirai Botnet Itself is Flawed; Hacking Back IoTs Could Mitigate DDoS Attacks, www.thehackernews.com/2016/10/mirai-botnet-iot-malware.html

[4] Mohit Kumar: *An Army of Million Hacked IoT Devices Almost Broke the Internet Today*, The Hacker News, www.thehackernews.com/2016/10/iot-dyn-ddos-attack.html

[5] Saját készítésű ábra

[6] Sérülékenység vizsgálat (Etikus Hack), www.itsecure.hu/etikus_hack

[7] Sándor Barnabás: *Közbeékelődéses támadás vizsgálata vezeték nélküli hálózaton* – Óbudai Egyetem, BGK, Tudományos Diákköri Dolgozat, 2017. április 19. ISBN 978-963-449-019-7

[8] Sean-Philip Oriyano: *CEH v9 Study Guide*, John Wiley & Sons Inc., Indianapolis, 2016, 129-145, ISBN 978-1-119-25224-5

[9] Khyati Jain: *Caution! Hackers Can Easily Hijack Popular Baby Monitors to Watch Your Kids*, The Hacker News, 2015.09.03., www.thehackernews.com/2015/09/baby-monitor-hacking-tool.html

[10] Swati Khandelwal: *FDA Recalls Nearly Half a Million Pacemakers Over Hacking Fears*, The Hacker News, 2017.08.31., www.thehackernews.com/2017/08/pacemakers-hacking.html